NSA - COMSEC

Army Regulation 530–2

Operations and Signal Security

Communications Security

Headquarters
Department of the Army
Washington, DC
1 September 1982

A Transition

This is the first step in publishing AR 530-2 as an UPDATE publication. Because the Baltimore Publication Center exhausted its supply of this publication, we chose to reprint the current material in the UPDATE format and at the same time incorporate any previously published permanent changes.

Over the next few years, all Department of the Army administrative regulations and many DA pamphlets will be converted to the UPDATE format. Some will appear as separate publications, like this one; others will be combined with related publications and will be published as handbooks like the All Ranks Personnel UPDATE.

The objective of UPDATE is to reduce the administrative burden on you, the user, and to improve the communications value of Army publications. Under UPDATE, a publication is printed at regularly scheduled times, and each printing includes all the changes made to the publication since its last printing. You might say that UPDATE publications are throw-away books; you simply discard the old issue when you get the new one. Under UPDATE, the "posting of changes" is a thing of the past.

Every UPDATE issue contains a Summary of Change. In the first printing of a book, the summary outlines the major topics covered by the publication. In subsequent printings, the summary outlines the major changes that have been made to the publication. Look for this summary in the front of every issue. It should help you zero in on areas that need your immediate attention.

If you need additional copies of this reprinted publication complete DA Form 4569 (USAAGPC Requisition Code Sheet) and send it to the Baltimore Publications Center.

The Editors

SUMMARY of CHANGE

AR 530-2
Communications Security

This is a transitional reprint of this publication which places it in the new UPDATE format. Any previously published permanent numbered changes have been incorporated into the text.

UPDATE Change Highlighting

The two techniques shown below are used to help readers identify new changes in administrative publications.

UPDATE Cancel and Underscore Technique

1.	2.	3.
Original text as it appeared in the base publication:	*Change* text as it appears in a current UPDATE issue:	*Fresh* text as it will appear in the next UPDATE issue:
The quick brown fox jumped over the lazy dog.	The quick ~~brown~~ gray fox jumped ~~over~~ on the lazy dog.	The quick gray fox jumped on the lazy dog.

UPDATE Tint Technique

1.	2.	3.
Text as it appeared in the last UPDATE issue:	*Restructured change text* as it appears in this UPDATE issue:	*Fresh* text as it will appear in the next UPDATE issue:

Chapter 12
Reporting Equipment Ideas, Problems and Warranty Claims

12–1. General
This chapter tells you how to make and submit:
a. Warranty Claim Actions (WCAs).
b. Equipment Improvement Recommendations (EIRs).
c. Quality Deficiency Reports (QDRs).

12–2. Warranty Claim Actions
a. Purpose. DA Form 2407 is used to send in WCAs for items with bad components, parts, or assemblies covered by a factory warranty. DA Form 2407 is also used to get payment for labor used replacing the bad items.
b. Identity of end items under warranty is shown by a decal plate, data plate, and labels.
c. All warranty actions, settled or not, are reported to the national level on DA Form 2407. Report local warranties settled with DA Form 2407 with the words "For Information only" written in block 16a. See Appendix F.

Chapter 12
Reporting Quality Deficiencies, Ideas, Equipment Improvement Recommendations and Warranty Claims

12–1. General
This chapter tells you how to make and submit:
a. Quality Deficiency Reports and suggest ideas and recommendations for improving equipment on the SF Form 368.
b. Warranty claim actions (WCA's) for items with bad components, parts, or assemblies covered by a factory warranty. Use the DA Form 2407 for WCA's.

12–2. Reporting Quality Deficiencies and Equipment Improvement Recommendations
a. The SF Form 368 is a multi-use form used for reporting:

Chapter 12
Reporting Quality Deficiencies, Ideas, Equipment Improvement Recommendations and Warranty Claims

12–1. General
This chapter tells you how to make and submit:
a. Quality Deficiency Reports and suggest ideas and recommendations for improving equipment on the SF Form 368.
b. Warranty claim actions (WCA's) for items with bad components, parts, or assemblies covered by a factory warranty. Use the DA Form 2407 for WCA's.

12–2. Reporting Quality Deficiencies and Equipment Improvement Recommendations
a. The SF Form 368 is a multi-use form used for reporting:

Distribution: There has been no special distribution made of this reprint issue. It is printed as a stock item for the Baltimore Publications Center. AR 530–2 distribution is B, C, D, E; for Active Army, D for ARNG, and D for USAR.

Subscription Information: This is a reprint of the current publication. Subscription cards are not inserted in this printing but will be inserted in the next printing.

Resupply: Limited copies of this UPDATE publication are available from the Baltimore Publications Center. Complete DA Form 4569 (USAAGPC Requisition Code Sheet) accordingly.

Locator Sheets: Until all publications are converted to the UPDATE format, the sequence of a "library" can be maintained by inserting this publication in the appropriate looseleaf binder where other publications are stored.

Editorial Comments: This UPDATE publication contains editorial comments that are not in the original standard version. These comments were inserted when there was a need to clarify the placement of an element of text (for example, the location of a referenced table). These comments are set in bold italic type and enclosed in parentheses.

Placement of Tables, Figures, Appendixes and "R" Forms:

- Full-page tables, figures and appendixes (in that order) in UPDATE publications are located after the last chapter of the related publication. Less than full-page tables and figures will be placed nearest the first cited reference in the publication.
- All reproducible forms (R forms) included in UPDATE publications are located at the back of the publication in numerical sequence beginning with DA Forms.

A Special Note About Forms and Local Reproduction: Forms are one of the Army's basic work tools. As the successful use of forms is closely related to the effective and efficient handling of personnel actions, the following general information about locally reproducible forms may be helpful to you:

- DA locally reproducible forms are designated with the suffix "R" as in DA Form XXXX-R.
- The authority for local reproduction of DD Forms and their use is given in the directive.
- Sources for forms not authorized for local reproduction are the AG publications centers or as stated in the authorizing directive. Since these forms may NOT be reproduced locally, they must be requisitioned.
- The copies of "R" forms at the back of publications printed in UPDATE are for your use in making local reproduction. Have them printed through your Forms Management Officer (FMO). In accordance with AR 310–1, paragraphs 4–26 and 4–28, the FMO may authorize the reproduction of a form in a modified format more convenient to local users. Those provisions permit back-to-back printing, carbon sets and continuous construction for word processing use.
- AR 310–1 also authorizes overprinting of locally fixed processing information. The idea behind this authorization to overprint is to reduce the amount of time a typist has to spend repeating local standardized requirements.
- The rules for procuring printing differs from place to place therefore, your FMO may not be able to approve the printing. In such a case the decision to overprint, or not to overprint, locally required information would be made at the lowest level where printing decisions are made.

The forms and local reproduction program offers you an opportunity to reduce your administrative burden and to save precious manhours for your unit.

This is the signature of an Army UPDATE publication.

The relationship of pen and book in this mark depicts printed communications—ideas disseminated rapidly and accurately in an economically and aesthetically beneficial manner to serve and to be conveniently used by a large audience

Headquarters
Department of the Army
Washington, DC
1 September 1982

*Army Regulation 530–2

Effective 1 October 1982

Operations and Signal Security

Communications Security

The original form of this regulation was published on 1 September 1982. Since that time, Change 1 has been issued to amend the original, and this change remains in effect. This UPDATE issue is a reprint of the original regulation with the change incorporated directly into the text.

By Order of the Secretary of the Army:

E. C. MEYER
General, United States Army
Chief of Staff

Official:

ROBERT M. JOYCE
Major General, United States Army
The Adjutant General

Summary. This revision adds responsibilities for The Assistant Deputy Chief of Staff for Operations and Plans for Command, Control, Communications, and Computers; identifies support of the Army operations security (OPSEC) program as a communications security (COMSEC) objective; addresses foreign electronic warfare (EW) capabilities as a COMSEC threat; defines policy for record telecommunications security; adds authentication and transmission of national security information procedures. It also eliminates encrypt-for-transmission-only (EFTO) procedures.

Applicability. See paragraph 1–2.

Impact on New Manning System. See paragraph 1–2.1.

Supplementation. Local limited supplementation of this regulation is permitted but is not required. If supplements are issued, HQDA agencies and major Army commands will furnish one copy of each to HQDA(DAMO–C4T), WASH DC 20310; other commands will furnish one copy of each to the next higher headquarters.

Interim changes. Interim changes to this regulation are not official unless they are authenticated by The Adjutant General. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

Suggested Improvements. The proponent agency of this regulation is the Office of the Deputy Chief of Staff for Operations and Plans. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) direct to HQDA(DAMO–C4T), WASH DC 20310.

Distribution. To be distributed in accordance with DA Form 12–9A requirements for AR, Operations and Signal Security: Active Army: B, C, D, E; ARNG, USAR: D.

Contents (Listed by paragraph number)

*This regulation supersedes (C) AR 530–2, 3 March 1976; AR 380–26, 6 September 1965; and AR 380–51, 20 May 1974.

Chapter 1
General

1–1. Purpose
This regulation prescribes policy and responsibilities for communications security (COMSEC) in the Army. It implements the National Communications Security Directive and DoD Directive 5200.5. It also establishes authority for programing actions and provides guidance for implementing COMSEC measures and procedures. All Army publications which identify COMSEC responsibilities must conform to this regulation.

1–2. Applicability
a. This regulation applies to those elements of the Active Army, the Army National Guard (ARNG) and the US Army Reserve (USAR) responsible for—

(1) Combat developments involving the security of telecommunications.

(2) Conducting research, development, test, and evaluation (RDTE) of telecommunications and COMSEC equipment.

(3) Providing technical guidance to and maintaining cognizance of COMSEC programs and activities.

(4) Computing quantitative requirements for COMSEC material; programing and budgeting for COMSEC material; and producing, procuring, distributing, supporting, maintaining, and disposing of COMSEC material.

(5) Planning, installing, operating, supporting and maintaining cryptofacilities.

(6) Conducting military operations.

(7) Training individuals in the operation and maintenance of COMSEC equipment or systems and incorporating COMSEC into unit training.

(8) Controlling and accounting for COMSEC material.

b. **Rescinded.**

1–2.1. Impact on New Manning System
This regulation does not contain information that affects the New Manning System.

1–3. References
Required and related publications are listed in appendix A.

1–4. Explanation of abbreviations and terms
Abbreviations and special terms used in this regulation are explained in the glossary.

1–5. Secure communications
a. The security of Federal telecommunications is a national responsibility. The activities assigned this responsibility must satisfy the requirements of the National Security Council (NSC) and the departments and agencies of the Federal Government.

b. The Secretary of Defense (SECDEF) is the US Government's Executive Agent for COMSEC. The Director, National Security Agency (DIRNSA) acts for the SECDEF in a wide range of COMSEC matters concerned with the security of Federal telecommunications.

c. Telecommunications of all types are vulnerable, in some degree, to intercept and to exploitation by hostile communications intelligence (COMINT). Encrypted telecommunications and telecommunications transmitted via protected distribution systems (PDS) are less subject to exploitation for intelligence purposes. However, transmissions over the encrypted radio link portion of a communications system remain vulnerable to interception and to direction finding and jamming. Inadequately protected telecommunications are lucrative sources of information to foreign intelligence collection activities.

d. The purpose of COMSEC is to protect telecommunications from foreign exploitation and to insure the authenticity of such communications. Encryption in an approved cryptosystem and radio silence are the best defenses against foreign COMINT efforts. Other COMSEC measures include—

(1) PDS

(2) Authentication.

(3) Proper operator skills and discipline.

(4) Appropriate user training.

(5) COMSEC awareness.

(6) Command emphasis on COMSEC matters.

e. COMSEC measures that are effective today may not be adequate in the future because of advances in COMINT technology. Therefore, COMSEC measures in use must be continuously evaluated. This is necessary to identify weaknesses which may be exploitable within the useful life of the information transmitted.

1–6. Communications intelligence capabilities
a. Most foreign countries engage in COMINT operations to meet their intelligence requirements. These COMINT efforts are assumed to be commensurate with the countries' technical competence or access to technical assistance. Such efforts involve intercepting and exploiting unprotected or inadequately protected communications. They may range from highly sophisticated operations capable of extracting useful information from all types of transmissions to a simple capability of intercepting clear text voice transmissions.

b. Foreign COMINT efforts operate continuously. These efforts are directed against those telecommunications systems that produce the most useful and timely intelligence. As use of encryption increases, foreign collection activities will seek to employ other techniques. This may include—

(1) More comprehensive coverage of remaining clear text transmissions.

(2) Obtaining keying material by covert means.

(3) Exploiting compromising emanations.

(4) Placing more emphasis on information derived from radio direction finding, signals analysis, radio fingerprinting, and operator identification techniques.

c. The composite of all information available through collection techniques is extremely important to the international relations and military planning of foreign countries. Determined efforts to obtain intelligence information from US telecommunications will continue as long as it is technically feasible to overcome the COMSEC effort and achieve acceptable levels of success.

d. It is assumed that the worldwide foreign intelligence effort provides extensive COMINT coverage of all Army telecommunications. This includes nontactical and tactical telecommunications in CONUS and overseas. Also, the nature and scope of COMINT coverage will change as intelligence requirements change. During periods of normal international relations, the COMINT coverage may be limited and highly selective. During periods of military exercises or increased international tension, the COMINT coverage may be expanded to exploit COMSEC weaknesses.

e. COMINT successes result from technical competence, operational resources, and opportunity (COMSEC weaknesses). Technical competence and operational resources are supplied by the enemy. Opportunity is supplied by the victim. Therefore, the telecommunications user can and must reduce the potential for the COMINT success of an enemy.

f. Classified COMINT threat information is available. Requirements for this information should be forwarded to HQDA(DAMI–FI), WASH DC 20310.

1–7. Electronic warfare capabilities
Enemy forces in a hostile tactical environment will employ electronic warfare (EW) and tactical weaponry to selectively disrupt (jamming and deception) or destroy command, control, and weapon communications systems. Enemy electronic warfare support measures (ESM) identify, locate, and prioritize valuable friendly targets for electronic counter measures (ECM) or destruction. For example, Soviet doctrine advocates the use of EW as an element of combat power. It is certain that electromagnetic radiations emitted by most tactical command and control communications systems will subject those systems to jamming or destruction.

a. Jamming may cause friendly operators to change to a less secure communications means, thereby reducing the security of the information being passed.

b. Imitative electronic deception can result in passing sensitive information to hostile elements which intrude into friendly nets.

c. Good COMSEC procedures will reduce the effectiveness of hostile ESM by making it more difficult to select targets for ECM.

1–8. Army COMSEC objectives
The Army's COMSEC goal is to provide total security for all electrically transmitted

information from the originator to the recipient. Objectives supporting this goal are as follows:

a. Insure that all military voice radio systems will be secured. (See para 1–9*a*).

b. Insure that COMSEC policy, plans, programs, budgets, and materiel life-cycle management are directed toward a fully coordinated and effective Army COMSEC effort.

c. Provide total cryptographic security or a PDS for electrical transmission of all classified information.

d. Provide cryptographic protection or a PDS for electrical transmission of unclassified national security related information.

e. Provide effective defense against interception, traffic analysis, and imitative communications deception by using transmission security practices.

f. Protect COMSEC material and COMSEC information from compromise.

g. Emphasize COMSEC awareness and training by routinely using all available COMSEC capabilities during day-to-day activities.

h. Conduct and plan the RDTE, procurement, and distribution of telecommunications and related COMSEC equipment and associated installation or adapter kits to insure their concurrent availability.

i. Reduce the cost of COMSEC equipment developed for Army applications.

j. Reduce or eliminate, to the extent possible, the security classification of and accounting controls for COMSEC equipment and material at the tactical level.

k. Support the Army operations security (OPSEC) program as outlined in AR 530–1.

l. Support the National COMSEC Assessment Program in accordance with DOD Directive 5200.5.

1–9. Policy

COMSEC will be an integral part of Army planning, programing, engineering, and operations.

a. All military voice radio systems will be secured or securable by an approved cryptosystem.

(1) In the absence of a machine encryption capability, manual cryptosystems will be used to provide the requisite security.

(2) All future military radios intended for the inventory will be developed, procured, and deployed for operational use as either secured or securable equipment.

b. Further procurement of radios presently in the inventory will be limited to those which are either secured or securable.

c. Excluded from the securable radio policy are radios used to relay traffic all of which is encrypted and decrypted at terminals remote from the radio itself. These are multichannel radios that receive and transmit only encrypted signals.

d. All record telecommunications will be secured by either encryption in approved cryptosystems or by PDSs. Record telecommunications is the telecommunications or teleprocessing of record information.

e. During electrical transmissions, all classified information will be provided cryptographic security unless the following occurs:

(1) The information is transmitted in the clear over a PDS as authorized in appendix B.

(2) Emergency conditions exist as specified in appendix B.

f. Off-line cryptosystems (machine and manual codes and ciphers) will be used to protect classified information over nonprotected distribution systems and over those telecommunications systems not secured by on-line machine cryptosystems.

g. Authentication systems will be used to provide a defense against imitative communications deception and to establish the authenticity of stations, communicators, or communications. (See app C.)

h. Only hardcopy keying material produced by National Security Agency (NSA) and cryptoequipment approved by the NSA will be used. In an emergency, the US Army Intelligence and Security Command (INSCOM) may produce and distribute hardcopy keying material (para 2–10*h*). Local production of hardcopy keying material by non-INSCOM activities is prohibited.

i. COMSEC will be an integral part of the planning and conduct of unit training and day-to-day operations at all levels of command. Full use will be made of available cryptosystems (machine and nonmachine) during training.

j. The application of COMSEC will be continuous throughout the life-cycle management and operation of telecommunications equipment.

k. COMSEC equipment developed for the Army should be small, reliable, and lightweight. All such equipment should be low-powered, unclassified when not keyed, and capable of operating in the required operational environment. No significant operational, environmental, or power requirements should be imposed on communications systems by COMSEC equipment.

l. COMSEC will be achieved with no more than a minimal increase in the frequency bandwidth required by the basic telecommunications equipment.

m. Commercially developed privacy or security equipment using the DES or a commercial algorithm will not be used to protect or encrypt any form of classified information within the Army. The only exception to this will be when prior approval has been obtained from HQDA (DAMO–C4T) WASH DC 20310. The unauthorized use of such devices to encrypt and transmit classified information will be considered a case of clear text transmission and a violation of military security.

n. Unclassified national security–related information of value to an adversary transmitted by and between Government elements and contractors will be given communications protection commensurate with the associated risk of exploitation. For this purpose maximum use will be made of those telecommunications systems that either—

(1) Have an on-line machine encryption capability.

(2) Use PDS.

(3) Use commercial communications protection equipment.

o. US Army commands and agencies may procure and use NSA approved commercial cryptographic equipments and techniques to satisfy communications protection requirements for unclassified information, except in some significant risk situations where other communications protection measures may be prescribed.

p. Only commercial communications protection equipment that meets Federal Standard 1027 will be considered by Army commands and agencies. Approval of the use of this equipment, using the Data Encryption Standard (DES) or a commercial algorithm, for the protection of unclassified national security related or sensitive information will be obtained from HQDA(DAMO–C4T) WASH DC 20310 on a case-by-case basis. Army commands and agencies desiring to procure and use commercially available hardware must forward their requests through appropriate channels to HQDA(DAMO–C4T) with the following information:

(1) Identification of equipment by manufacturer and model name or number.

(2) Intended purpose or proposed application.

(3) Type of unclassified information to be protected and an assessment of whether the information to be protected during transmission is national security related.

(4) Approximate length of time the information needs to be protected.

(5) Adversary or adversaries against whom the protection is desired.

(6) An assessment, from the user's standpoint, of the risk of exploitation of the information by an adversary.

q. Only NSA approved keying material will be used with the commercial communications protection equipment approved for Army use. Requirements for keying material will be submitted as required by TB 380–41.

r. All exceptions to the general policy of secure communications for voice radio or record telecommunications must be approved by HQDA(DAMI–CIC) WASH DC 20310.

Chapter 2
Responsibilities

2–1. Deputy Chief of Staff for Operations and Plans (DCSOPS)

The DCSOPS has general staff responsibility for the development of strategic concepts, estimates, plans, and broad base requirements in accordance with AR 71–9. In discharging this responsibility, the DCSOPS will—

a. Monitor Army Staff actions involving COMSEC.

b. Monitor training activities to insure that proper emphasis is given to COMSEC during training conducted at all levels.

c. In matters involving Army combat developments—

(1) Approve COMSEC studies, concepts, and proposed doctrine.

(2) Insure that COMSEC doctrine is integrated into overall Army doctrine.

(3) Approve operational capability objectives (OCOs), letters of agreement (LOAs), and required operational capabilities (ROCs) for COMSEC equipment. Establish priorities for the RDTE effort.

(4) Insure that realistic and essential COMSEC requirements are included in OCOs and material requirement documents for telecommunications equipment.

(5) Insure allocation of enough manpower to accomplish essential COMSEC functions.

(6) Insure that adequate COMSEC instruction is included in appropriate individual training programs at Army training centers and at Army Service schools.

d. When establishing requirements for the use of Army forces—

(1) Insure integration of COMSEC into OPSEC planning and practices.

(2) Set operational priorities, considering both operational and security requirements, for worldwide distribution of COMSEC equipment.

2–2. Assistant Deputy Chief of Staff for Operations and Plans for Command, Control, Communications, and Computers (ADCSOPS(C4))

The ADCSOPS(C4) has general staff responsibility for the overall management of Army COMSEC activities. As part of this responsibility, ADCSOPS(C4) will—

a. Serve as the principal Army Staff point of contact to The Office of the Secretary of Defense (OSD), the Joint Chiefs of Staff, NSA, and other military departments on COMSEC matters.

b. Insure the development and execution of coordinated programs to achieve Army COMSEC goals and objectives.

c. Develop and disseminate HQDA COMSEC resources programing guidance. Provide this guidance to major Army commanders and to directors of the Army RDTE and procurement appropriations reflecting COMSEC resources.

d. Review COMSEC-related program elements. This will insure that the COMSEC operations and maintenance, Army (OMA) portions are consistent with the HQDA COMSEC programing guidance.

e. Justify and defend COMSEC budget requirements contained in the COMSEC Resources Program (CRP).

f. Review the usage of COMSEC resources by major Army commands (MACOMs) and provide guidance as required.

g. Represent the Secretary of the Army on the National Communications Security Committee (NCSC).

h. Prepare the Army report to the NCSC on the status of COMSEC as directed by the NCSC.

i. Include COMSEC considerations as an integral part of telecommunications systems planning and programing.

j. Monitor telecommunications and COMSEC concepts and doctrine for conformance to establish COMSEC policies and standards.

k. Review Army, joint, and combined telecommunications plans to insure that provisions for COMSEC are adequate and conform to established COMSEC policies and standards.

l. Review and approve the basis of issue plan (BOIP) for COMSEC equipment to insure that the proposed distribution and type of equipment are compatible with the telecommunications systems.

m. Establish priorities for procurement of COMSEC equipment.

n. Review COMSEC requirements, plans, and programs, including RDTE, to insure supportability from a frequency management standpoint.

o. Assist Deputy Chief of Staff for Research, Development, and Acquisition (DCSRDA) in justifying and defending programs and budget requirements for COMSEC RDTE and procurement.

p. Approve commercial communications protection equipment for Army use.

2–3. Assistant Chief of Staff for Intelligence (ACSI)

The ACSI has general staff responsibilities for intelligence, counterintelligence, and security activities. In discharging this responsibility, the ACSI will—

a. Provide evaluations of COMINT threats. Recommend levels of encryption, by priorities, and other measures to protect Army telecommunications from exploitation.

b. Prescribe the degree and kind of protection needed to safeguard national security and national security related information during electrical transmission.

c. Develop and implement COMSEC policies and standards to minimize intelligence exploitation to prevent unauthorized access to COMSEC material and to insure the physical security of cryptofacilities.

d. Provide staff supervision for COMSEC surveillance activities.

e. Authorize release of COMSEC material and information to foreign governments per AR 380–10.

f. Review existing and proposed COMSEC doctrine and Army ROCs. Make recommendations as appropriate.

g. Develop and implement policies and standards for the control and security accounting of COMSEC material.

h. Assist the ADCSOPS(C4) in justifying and defending program and budget requirements in support of COMSEC surveillance activities.

2–4. Deputy Chief of Staff for Logistics (DCSLOG)

The DSCSLOG has general staff responsibilities for development and supervision of the Army logistics system and for management of material and supplies. With respect to COMSEC, the DCSLOG will—

a. Develop logistics policies, including Integrated Logistics Support (ILS) policy, concepts, procedures, and guidance for distribution, supply, maintenance, and transportation of COMSEC equipment used in support of all Army telecommunications systems. This includes the Army portion of the Defense Communications System (DCS).

b. Prescribe execution of NSA or OSD logistics management directives that apply to COMSEC material.

c. Act as proponent of the Army COMSEC Commodity Logistics Accounting Information Management System (ACCLAIMS).

d. Prescribe and supervise the implementation of procedures for property control and the accounting of COMSEC material during distribution, storage, maintenance, use, and disposal. All guidance will conform with the policies and standards developed by the ACSI for safeguarding COMSEC material.

e. Supervise logistics support planning to insure the availability of material and publications needed for repair, test measurement, and diagnosis of COMSEC equipment.

f. Assist the ADCSOPS(C4) in justifying and defending program and budget requirements in support of COMSEC logistics functions.

2–5. Deputy Chief of Staff for Personnel (DCSPER)

The DCSPER has general staff responsibility for the development and administration of the military personnel management system. As this relates to COMSEC, the DCSPER will—

a. Manage COMSEC personnel resources to meet approved manpower requirements.

b. Provide career development opportunities for COMSEC personnel to fill key COMSEC positions.

c. In comformance with policies and standards developed by the ACSI prescribe measures for physical security exterior to the walls of cryptofacilities and assure integration of those measures into command and physical security plans.

d. Review materiel requirements documents for physical security equipment used to safeguard COMSEC material at fixed installations in the continental United States (CONUS) and outside the continental United States (OCONUS).

2–6. Deputy Chief of Staff for Research, Development, and Acquisition (DCSRDA)

The DCSRDA has general staff responsibilities for RDTE and procurement of material

from concept formulation through production acceptance testing (AR 70–1). With respect to COMSEC, the DCSRDA will—

a. Develop, coordinate, and allocate RDTE and procurement resources in support of the CRP. Supervise the execution of RDTE and procurement.

b. Justify and defend program and budget requirements for COMSEC RDTE and procurement.

c. Serve as the Other Procurement, Army (OPA) appropriations director for COMSEC material.

d. Forward to the NSA HQDA-approved materiel requirement documents for COMSEC equipment along with requests for RDTE efforts to fulfill those needs. Designate an Army developing agency to monitor development and to insure that Army material life-cycle management milestones are satisfied.

e. Monitor planned COMSEC RDTE projects which are of interest to the Army, but are conducted by NSA or another military department. Designate an Army developing agency as defined in AR 70–1 for each project having potential application for Army use. Insure that the designated agency conducts liaison with the developer and keeps interested Army agencies informed of the progress of such projects.

f. Insure, in coordination with NSA, the development of COMSEC equipment and any companion telecommunications equipment at the same time. RDTE of related equipment should have concurrent life-cycle management milestones from concept formulation through production acceptance testing.

g. Provide the primary Army member for the NSA COMSEC Research and Engineering Coordination (CREC) Group.

h. Serve as RDTE appropriations director for COMSEC material.

2–7. Commanding General, US Army Training and Doctrine Command (CG, TRADOC)

The CG, TRADOC is responsible for Army combat development activities and for Army individual training programs. In discharging these responsibilities, the CG, TRADOC will—

a. Integrate approved COMSEC doctrine, material, and techniques into the instructional programs of Army service schools for which TRADOC is responsible.

b. Train individuals in COMSEC awareness and in the operation, maintenance, and safeguarding of COMSEC material.

c. Develop and insure that COMSEC training literature to support individual and unit training programs is included in the TRADOC portion of the Army-wide Training Literature Program. Coordinate with the other MACOMs to insure the compatibility of COMSEC training literature with current unit training needs and programs.

d. Include COMSEC as a subject to be evaluated during written and performance testing of the soldier in Army individual training and in the annual skill qualification test.

e. Develop training aids and training films for COMSEC equipment and support of Army-wide COMSEC training and awareness programs.

f. Insure that all Army-wide training literature issued by TRADOC includes COMSEC considerations.

g. Insure that major Army commanders are advised regularly of changes in COMSEC doctrine, techniques, material, and procedures for their use in discharging command COMSEC responsibilities.

h. Develop, test as directed, and recommend to the DCSOPS (DAMO–C4T), WASH, DC 20310, operational and organizational concepts and doctrine to meet COMSEC goals and objectives for the Army.

i. Develop OCOs and material requirements documents to meet the COMSEC requirements of the Army in the field and submit them to the DCSOPS (DAMO–C4T) WASH DC 20310.

j. Review and evaluate material requirement documents developed by other commands to see if they represent a valid COMSEC need for the Army.

k. Before being forwarded to the DCSOPS, coordinate material requirements documents prepared by Army elements for COMSEC equipment with—

(1) DIRNSA.

(2) US Army Communication Command (USACC).

(3) US Army Materiel Development and Readiness Command (DARCOM).

(4) INSCOM.

(5) Other MACOMs, as appropriate.

l. Coordinate the following with INSCOM—

(1) Training and doctrinal literature including programs of instruction.

(2) Training films.

(3) OCOs.

(4) Operational and organizational concepts and procedures.

(5) Material requirement documents for telecommunications or COMSEC equipment.

m. As directed, plan for and conduct operational testing of COMSEC equipment to be used by the Army in the field. Assure early coordination of operational test plans with the MACOM designated to provide test forces. The cryptonetting philosophy to be used during the operational testing of COMSEC equipment must be coordinated with and approved by INSCOM.

n. Together with INSCOM, and other MACOMs as appropriate, develop and recommend to DCSOPS the BOIP for COMSEC equipment to be used by the Army in the field.

o. Insure that COMSEC tasks, conditions, and standards appear in unit evaluation programs.

2–8. Commanding General, US Army Materiel Development and Readiness Command (CG, DARCOM)

The CG, DARCOM has responsibility for providing material and related logistics services. With respect to COMSEC, the CG, DARCOM will—

a. Together with NSA, conduct RDTE of COMSEC techniques to increase the future COMSEC capability of Army equipment.

b. Together with DCSRDA, conduct liaison with NSA and other military departments conducting COMSEC RDTE. Advise DCSRDA of any planned projects that have potential application for use by the Army in the field and insure that interested Army agencies are informed of the progress of ongoing projects.

c. Perform those material developer and ILS support functions prescribed for nondevelopment items (NDI) of COMSEC equipment developed by NSA which have Army application.

d. Perform the functions of a developing agency (AR 70–1) for COMSEC surveillance equipment.

e. Conduct RDTE of COMSEC equipment when the RDTE responsibility is assigned to the DA.

f. Advise, assist, and provide system engineering support to agencies regarding COMSEC aspects during their RDTE of telecommunications equipment and weapons systems.

g. Together with ACSI and INSCOM, prepare COMSEC guidance on the safeguards to be applied during a developmental or operational test. This guidance will accompany pertinent proposed material requirements documents.

h. In accordance with AR 70–61, initiate classification or reclassification of COMSEC equipment for which DARCOM is the developing agency.

i. Review BOIPs for COMSEC equipment and accomplish those DARCOM responsibilities assigned in AR 71–2.

j. Develop and provide criteria, instructions, and installation kits for integration of COMSEC equipment (developed or managed by DARCOM) with telecommunications systems.

k. Prepare the DARCOM input to the CRP and submit the input thru HQDA(DAMA–CSC) to HQDA(DAMO–C4R), WASH DC 20310.

l. Exercise COMSEC commodity management by—

(1) Operating the National Inventory Control Point (NICP) per AR 710–1 and the National Maintenance Point (NMP) per AR 750–1 as part of the COMSEC wholesale supply and maintenance system.

(2) Acting as the assigned responsible agency for the Class A1 multicommand standard ACCLAIMS.

(3) Conducting maintenance support planning, per AR 750–1, for all COMSEC material.

(4) Conducting new equipment training per AR 350–35.

(5) Providing technical assistance to users of COMSEC equipment per AR 700–4.

(6) Recommending to the Commanding General, US Army Military Personnel Center, per AR 611–1, new MOSs and changes to existing MOSs required to maintain COMSEC equipment. Developing human engineering factors per AR 602–1.

(7) Managing the COMSEC Material Control System per AR 380–40 and TB 380–41. This includes operation of the Army COMSEC Central Office of Record.

(8) Announcing compromises of COMSEC material when directed by the controlling authority and taking emergency resupply actions as required.

(9) Announcing the identification and supply availability of COMSEC keying material which is regularly superseded.

(10) Together with the appropriate military departments, federal agencies, and foreign governments, distributing keying material for joint and combined cryptonets.

(11) Together with INSCOM, conducting annual keying material reviews per AR 380–40 and TB 380–41.

(12) Granting relief from security accountability for COMSEC material accountable to the Army COMSEC Central Office of Record (ACCOR) per AR 380–40.

(13) Consolidating all Army COMSEC equipment requirements. Stratify these requirements for OPA programing in the CRP.

(14) Managing the COMSEC Equipment Modification Application Reporting System (CEMARS).

(15) Providing COMSEC logistics assistance to Army commanders worldwide.

(16) Providing NSA with the Army quantitative requirements for COMSEC keying material. Insure the availability of such material, consistent with operational and contingency requirements of the Army.

(17) Reviewing plans and directives having COMSEC logistics implications. Insure the adequacy for logistics support and adherence to established COMSEC logistics policy.

(18) Developing Army ILS requirements and conducting ILS planning for new COMSEC acquisition programs.

(19) Operating and maintaining the COMSEC Equipment Asset Reporting System (CEARS).

(20) Coordinating with the other Services and DoD Agencies, as appropriate, to develop standard logistics procedures for COMSEC material.

(21) Accounting for sealed authentication system per JCS Pub 13.

m. (U) Coordinate command-developed technical literature for telecommunicatcns or COMSEC equipment and systems with INSCOM.

2–9. Commanding General, US Army Communications Command (CG, USACC)

The CG, USACC is responsible for engineering, installing, operating, and maintaining the Defense Communications System (Army), air traffic control/navigation aids, and assigned Army Telecommunications systems. The CG, USACC will—

a. Develop and operate the assigned Army in the field COMSEC Logistics System in support of Army Component commands and unified commands.

b. Assist in the development and review of concepts, studies, and regulations which concern or affect COMSEC logistics functions for the Army in the field.

c. Prepare the USACC Operations and Maintenance (O&M) portion of the CRP and submit it to HQDA(DAMO–C4R) WASH DC 20310.

d. Prepare requirements for COMSEC material for inclusion in the OPA portion of the CRP and in the production forecasts for COMSEC aids. Submit these requirements to DARCOM (US Army COMSEC Logistics Activity, Ft Huachuca, AZ 85613).

e. Together with TRADOC and DARCOM, conduct liaison with NSA and other military developments conducting COMSEC RDTE. Advise DCSRDA (DAMA–CSC) WASH, DC 20310 of any planned projects which have potential application for use by USACC.

f. Perform operational tests and evaluations per AR 70–10 and AR 71–3 when designated as the operational tester.

g. Develop and recommend to TRADOC the BOIP for COMSEC equipment for which USACC Table of Organization and Equipment (TOE) units of the theater Army are intended users.

h. Insure that adequate COMSEC measures are applied and that approved COMSEC equipment requirements are reflected in telecommunications requirements (TELER). Coordinate TELER processed under AR 105–22 with INSCOM and the gaining major command.

i. Coordinate command-developed technical literature for telecommunications or COMSEC equipment and systems for DCS (ARMY) and assigned Army Telecommunications systems with INSCOM and DARCOM.

j. Provide input to TRADOC for COMSEC equipment training needs at the US Army Signal Center and School.

k. Insure compliance with paragraph 1–9*a* for those telecommunications systems engineered, installed, operated, and maintained by USACC. Request waivers from HQDA(DAMI–CIC) WASH DC 20310 as required.

2–10. Commanding General, US Army Intelligence and Security Command (CG, INSCOM)

The CG, INSCOM provides technical assistance in the application of, and adherence to Army COMSEC policies. The CG, INSCOM will—

a. Assist Army Staff and Army commanders at all levels, to include Reserve Components, in developing and evaluating COMSEC policies, plans, operating procedures, and training programs.

b. Advise Army Staff and Army Commanders at all levels, to include Reserve Components, in planning, coordinating, and implementing communications cover.

c. Review plans, directives, and training and doctrinal material, including training films and programs of instruction. Review OCOs, O&O concepts, material requirements documents, and BOIPs having COMSEC implications. Insure the adequacy of COMSEC considerations and adherence to established COMSEC policy.

d. Conduct COMSEC surveillance operations in support of Army commands and agencies (both Active and Reserve Components) at echelons above corps (EAC). Augment COMSEC surveillance capabilities of Army commands at echelons corps and below, as required. Perform analysis to determine the effectiveness of COMSEC applications.

e. Approve requests for the establishment, alteration, or relocation of Army cryptofacilities and other cryptofacilities as directed by HQDA.

f. Conduct inspections of all Army and other specified cryptofacilities per AR 380–40.

g. Recommend, from a security standpoint, NSA-produced COMSEC material for use within the Army.

h. Produce COMSEC keying material when the Army is authorized such production. This includes codes, nonmachine ciphers, authentication systems, and other cryptographic and transmission security aids.

i. Review and approve operational, contingency, and training cryptonets and cryptonetting philosophies contained in newly developed operational concept documents. Insure that cryptonetting is consistent with sound COMSEC principles.

j. Evaluate reports of physical and cryptographic insecurities.

k. Establish security criteria for disposal of Army COMSEC material.

l. Exploit foreign cryptologic information for COMSEC purposes.

m. Participate in preparation of studies concerning intelligence threats and operational vulnerabilities against which COMSEC must be provided.

n. Recommend COMSEC doctrine to TRADOC. As required, participate in combat development of doctrine relating to COMSEC. This will insure compatibility with COMSEC policy.

o. Recommend materiel requirements and BOIP for COMSEC surveillance equipment to TRADOC.

p. Exercise technical control by prescribing and promulgating technical procedures for the conduct of COMSEC surveillance operations. Monitor, through coordination with other MACOMs, the application and

implementation of these technical procedures.

q. Assist HQDA in evaluating the status of COMSEC Army-wide.

r. Manage the Army COMSEC Assessment Program; represent the Army on National COMSEC Assessment Program Working Groups and panels as directed by HQDA.

s. Maintain liaison with COMSEC surveillance activities of other Services and DoD agencies to monitor and evaluate COMSEC surveillance policies and procedures for Army applications.

t. Inspect and certify those Automatic Secure Voice Communications (AUTOSEVOCOM) terminals which are under the jurisdiction of DA.

u. Prepare the INSCOM portion of the CRP and submit it thru HQDA(DAMA-CSC) to HQDA(DAMO-C4R), WASH DC 20310.

2-11. Commanding General, US Army Forces Command (CG, FORSCOM); Commanding General, US Army Europe; Commanding General, US Army Western Command (CG, WESTCOM); Commanding General, Eighth Army; and the Chief, National Guard Bureau (CNGB)

These are responsible for maintaining the combat readiness of assigned and attached troop units. Assigned troop units for FORSCOM and WESTCOM include Active Army and USAR units. With respect to COMSEC, they will perform the following:

a. Review material requirements documents for COMSEC equipment, develop material requirements to support unit training, and recommend to TRADOC that these requirements be included in the material requirements documents.

b. Introduce and integrate approved COMSEC doctrine, material, and techniques into the unit training programs.

c. Direct the application of unit COMSEC training tasks, conditions and standards to all assigned and attached units.

d. Insure that sufficient COMSEC accounts are established and that necessary COMSEC material is issued to assigned and attached units. This is done to insure that training and mobilization requirements are met.

e. As required, participate with TRADOC activities in combat development studies and force development testing and experimentation (FDTE) of concepts and in the development of doctrine relating to COMSEC. As directed, support FDTE developmental and operational tests of COMSEC material.

f. Monitor COMSEC surveillance activities of assigned and attached COMSEC support units. Assist INSCOM in the Army COMSEC assessment program by providing information requested in response to national COMSEC assessment program requirements.

g. Monitor the command cryptofacility inspection programs of subordinate units conducted in accordance with AR 380-40 and TB 380-41.

2-12. Commanding General, US Army Health Services Command (CG, HSC)

In discharging responsibilities for medical combat development activities and training of medical personnel, the CG, HSC will—

a. Introduce and integrate approved COMSEC doctrine, material, and techniques into the following programs:

(1) Instructional programs of CONUS Army HSC schools.

(2) Training programs for medical personnel and units.

b. Include COMSEC tasks, conditions, and standards in the evaluation programs of medical units.

2-13. Commanding General, US Army Operational Test and Evaluation Agency (CG, OTEA)

The CG, OTEA is responsible for managing all user testing, operational tests (OT), FDTE, and joint user tests directed by OSD. In discharging this responsibility, the CG, OTEA will—

a. Plan, budget for, and conduct OT or FDTE of COMSEC equipment assigned for testing.

b. For assigned testing, coordinate with INSCOM to assure COMSEC aspects are adequate.

c. Provide an independent evaluation of tested COMSEC material to the appropriate decision body at major system milestones.

2-14. Commanders at all levels

In planning, programing, and providing resources for COMSEC activities, commanders will—

a. Designate staff responsibilities for planning, supervising, and evaluating command COMSEC activities. (See TB IG 1 for guidance on evaluating command COMSEC activities.)

b. Insure that associated telecommunications equipment is on hand or on order before requisitioning COMSEC equipment.

c. Use only hardcopy keying material produced by NSA or INSCOM. Insure the proper use of this material.

d. Obtain INSCOM approval for command cryptofacilities per AR 380-40.

e. Appoint COMSEC custodians. Insure that the COMSEC material is accounted for per TB 380-41.

f. Maintain adequate COMSEC surveillance of command telecommunications by the supporting signal security (SIGSEC) element (organic tactical and INSCOM EAC). Insure that COMSEC surveillance activities contribute to a continuing assessment of the effectiveness of the command COMSEC effort.

g. Insure that the protection of COMSEC material conforms to DA standards. Include cryptofacilities in command physical security plans.

h. Insure that command cryptofacility inspections are conducted per AR 380-40 and TB 380-41.

i. Insure that appropriate emphasis is placed on COMSEC in unit training, command school programs, and training exercises.

j. Insure responsive logistics support for the effective application of COMSEC material in their commands. Insure that this logistics support includes timely application of COMSEC equipment modifications and modification reporting as specified in AR 380-40 and TB 380-41.

k. When performing controlling authority functions as required by AR 380-40—

(1) Provide for COMSEC compatibility in planning cryptonets for which the commander is the controlling authority; determine requirements for COMSEC keying material, and inform the appropriate COMSEC distribution authority.

(2) Announce effective editions of all keying material to be used in cryptonets for which the commander is the controlling authority.

(3) In accordance with TB 380-41, evaluate reports of lost, missing, or unaccounted for COMSEC keying material used in cryptonets for which the commander is the controlling authority. As required, declare compromises; notify responsible agencies, and conduct appropriate investigations.

(4) Take actions specified in AR 380-40 and TB 380-41 for lost, missing, or unaccounted for COMSEC material.

l. Prior to publications, submit copies of plans, directives, and unit training material having COMSEC implications to the supporting or organic SIGSEC element. This element will review the adequacy of COMSEC considerations and adherence to COMSEC policy.

m. Make maximum use of all available COMSEC systems (machine and manual). Operational and training after-action-reports will specifically include all instances of failure to use available COMSEC systems.

n. Incorporate the provisions of the COMSEC Penalty Assessment Program (FM 105-5) during training exercises, tests, and similar training activities to improve COMSEC field training.

o. Establish and operate aggressive net control station procedures in all radio communications. Include COMSEC in all radio operator training on proper net and radio procedures to insure communications discipline and adherence to approved COMSEC practices.

p. Improve telephone security by providing visibility for the present secure telephone system as shown below:

(1) Add secure telephone numbers to the organization or department locator charts.

(2) Add secure telephone numbers to the organization section of the telephone directory.

(3) Insure that all personnel are aware when AUTOSEVOCOM service is available and provide ready access to the DCS AUTOSEVOCOM directory.

(4) Continually remind all personnel of the availability, location, and telephone

numbers of the AUTOSEVOCOM and other secure telephone terminals.

q. Implemement the Army Communications-Electronics Operation Instructions (CEOI) Program in accordance with AR 105–64.

r. Insure compliance with paragaph 1–9*a* for all assigned telecommunications systems. Request a waiver from HQDA, ATTN: DAMI–CIC; WASH, DC 20310, for those telecommunications systems where compliance is infeasible.

s. Prescribe measures to be taken to secure the exterior of cryptofacilities, per AR 190–13.

t. Insure that DD Form 2056 (Telephone Monitoring Notification Decal) 1 December 76, is applied to all nontactical unsecured telephone instruments.

u. Insure unclassified national security related information and sensitive information is provided adequate protection during transmission.

v. Insure adequate security or protection is provided for all command telecommunications per paragraph 1–9 above.

Appendix A
References

Section I
Required Publications

AR 70–1
Army Research, Development and Acquisition. (Cited in paras 2–6 and 2–8.)

AR 70–10
Test and Evaluation During Development and Acquisition of Materiel. (Cited in para 2–9.)

AR 70–61
Type Classification of Army Materiel. (Cited in para 2–8.)

AR 71–2
Basis of Issue Plans. (Cited in para 2–8.)

AR 71–3
User Testing. (Cited in para 2–9.)

AR 71–9
Materiel Objectives and Requirements. (Cited in para 2–1.)

AR 105–22
Telecommunications Requirements Planning, Developing, and Processing. (Cited in para 2–9.)

AR 105–64
US Army Communications Electronics Operation Instructions (CEOI) Program. (Cited in para 2–14.)

AR 190–13
The Army Physical Security Program. (Cited in para 2–14.)

AR 350–35
New Equipment Training. (Cited in para 2–8.)

AR 380–10
Department of the Army Policy for Disclosure of Military Information to Foreign Governments (U). (Cited in para 2–3.)

(C) AR 380–40
Policy for Safeguarding and Controlling COMSEC Information (U). (Cited in paras 2–8, 2–10, 2–11, and 2–14.)

AR 530–1
Operations Security (OPSEC). (Cited in para 1–8.)

(S) AR 530–4
Control of Compromising Emanations (U). (Cited in para B–5.)

AR 602–1
Human Factors Engineering Program. (Cited in para 2–8.)

AR 611–1
Military Occupational Classification Structure Development and Implementation. (Cited in para 2–8.)

AR 700–4
Logistic Assistance Program. (Cited in para 2–8.)

AR 710–1
Centralized Inventory Management of the Army Supply System. (Cited in para 2–8.)

AR 750–1
Army Materiel Maintenance Concepts and Policies. (Cited in para 2–8.)

FM 105–5
Manuever Control. (Cited in para 2–14.)

(O) TB 380–41
Procedures for Safeguarding, Accounting and Supply Control of COMSEC Material. (Cited in paras 1–9, 2–8, 2–11, and 2–14.)

(C) TB 530–1
Identification and Application of Compromising Emanation Control Measures (U). (Cited in para B–5.)

(S) JCS Pub 13, Vol I
Policy and Procedures Governing the Authentication and Safeguarding of Nuclear Control Orders (U). (Cited in para 2–8.)

Section II
Related Publications

A related publication is merely a source of additional information. The user does not have to read it to understand this regulation.

AR 105–10
Communications Economy and Discipline

AR 105–31
Record Communications

AR 380–5
Department of the Army Information Security Program

AR 380–53
Telephone Communications Security Monitoring

AR 380–380
Automated Systems Security

(C) AR 530–3
Electronic Security (U)

AR 640–15
Criteria for Insuring the Competency of Personnel to Install, Maintain and Repair Communications Security Equipment

(C) DA PAM 310–9
Index to Communications Security (COMSEC) Publications (U)

(C) DA PAM 380–2
SIGSEC: Defense Against SIGINT (U)

(C) TB 380–7
Tempest Inspection and Test (U)

(C) TB 380–9
SIGSEC Survey Guide (U)

JCS Pub 1
Dictionary of Military and Associated Terms

(C) DoD Directive 5200.5
Communications Security
National Communications Security Directive (U), June 20, 1979

Appendix B
Clear Text Transmission of National Security Information

B–1. Purpose

This appendix prescribes DA procedures to be used for the unsecured electrical transmission of classified information during emergency situations. It also prescribes criteria under which PDS (formerly known as Approved Circuits) may be established and used for transmission of classified information under a variety of situations.

B–2. Emergency procedures

Secure communications systems that allow complete freedom and flexibility in the exchange of information are essential elements of military operations. However, emergency situations may arise when secure communications of any form are not available and immediate needs dictate the clear text electrical transmission of classified information.

a. Information classified TOP SECRET may not be electrically transmitted in-the-clear over unsecured means at any time. During hostilities, CONFIDENTIAL and SECRET information may be electrically transmitted in-the-clear by unsecured means (such as telephone, teletypewriter, and radio) as an emergency measure when all of the following conditions exist:

(1) The transmitting or receiving station is located in a theater of actual hostilities.

(2) Speed of delivery is essential.

(3) Encryption cannot be accomplished.

(4) Transmitted information cannot be acted upon by the enemy in time to influence current operations.

b. When CONFIDENTIAL OR SECRET information must be transmitted in-the-clear, according to paragraph *a*, the following procedures will be followed:

(1) Each transmission in-the-clear must be individually authorized by the commander of the unit or element transmitting the message or by his or her designated representative.

(2) References to previously encrypted messages are prohibited.

(3) The classification will not be transmitted as part of the message. Messages will be identified by the word "CLEAR" in place of the classification.

(4) Each transmission in-the-clear must be individually authenticated using an approved authentication system (transmission authentication).

(5) When "emergency in-the-clear" communications are received, record or other hard copy messages will be marked "RECEIVED IN-THE-CLEAR HANDLE AS CONFIDENTIAL" before delivery to the addressees. In-the-clear messages will be handled as CONFIDENTIAL material and will not be readdressed. Should an addressee determine that the information must be forwarded to another addressee, a new message will be originated, classified, and handled as the subject matter and situation dictate.

B–3. PDS

PDSs are a form of secure communications systems and augment encrypted communications. Such PDSs are afforded physical and electromagnetic safeguards to minimize the risk associated with communications cables carrying classified clear text information through unrestricted areas. Every practical effort should be made to install communications cables carrying clear text classified information entirely within restricted areas. Access to such cables should be limited to personnel cleared for the highest level of information the system will transmit. When portions of the cables must be installed in unrestricted areas, they must be under sufficient control (physical protection and/or surveillance) to preclude covert penetration and interception (tapping). PDSs include all equipment and cabling used for the clear text transmission of classified information. Prior to a PDS being used for the transmission of classified information, the PDS must be evaluated for compliance with the criteria in this appendix and be approved for the specific level of classified information to be transmitted.

B–4. PDS in multichannel telecommunications systems

a. COMSEC equipment to secure multichannel telecommunications systems has been entering the Army inventory for both fixed and tactical applications. This COMSEC equipment encrypts the information transmitted between the multiplexers of such systems and negates hostile intercept and exploitation. However, the interconnecting communications lines and cables which carry unencrypted classified information between the multiplexers and subscriber equipment must be protected.

b. By applying the fixed or tactical criteria in paragraphs B–5 and B–6, PDS may be used for securing communications lines between subscriber equipment and multichannel telecommunications systems secured by approved COMSEC equipment. In addition to the fixed or tactical criteria, the following criteria must also be met.

(1) Where PDSs are employed at both ends of a secured multichannel system, the approval authority for both PDSs will be the senior approval authority of the individual PDSs.

(2) The classification of information to be transmitted will not exceed the classification of the CRYPTO key securing the multichannel system.

(3) Procedures must be established for subscribers to report improper technical operations of the system. For example, cross talk problems on the PDS circuits must be reported to maintenance and security personnel for correction. Security personnel must promptly evaluate the security risk and, if the risk is unacceptable, remove the PDS from service until the problems have been corrected.

B–5. Fixed PDS

a. Authority to approve PDS for the clear text transmission of classified information within fixed plant and garrison installations is delegated as follows. This authority will not be further delegated.

(1) Heads of the Army General and Special Staff for activities under their staff supervision, direction, or control.

(2) MACOM commanders for their organic activities.

b. Before approval action is completed for fixed plant and garrison installations, approval authorities will coordinate with and obtain concurrence from the following if the PDS directly supports any of their elements or is within their security cognizance.

(1) Director, National Security Agency.

(2) Director, Defense Intelligence Agency.

(3) Director, Defense Communications Agency.

(4) Unified and Specified Commanders.

c. Approval authorities may request technical assistance from the INSCOM local support element in applying security criteria and processing the approval action. This assistance may include review and examination of any of the following:

(1) The physical security safeguards which will be maintained.

(2) Plans for installing and using the PDS.

(3) Adherence to the RED/BLACK installation criteria.

(4) The capability of the system to maintain the security required.

d. Approval actions for PDS to transmit TOP SECRET information must include an evaluation by the INSCOM local support element. Information copies of approvals for PDS to transmit TOP SECRET information, with all supporting documentation, will be forwarded to HQDA(DAMI–CIC), WASH DC 20310.

e. Once a PDS is approved, no changes in installation, additions, or use may be made until approval for such changes has been granted by the approval authority.

f. Fixed PDS must meet the following criteria:

(1) PDS will be located entirely within the limits of the installation under the using commander's physical control.

(2) Security techniques for PDS will be evaluated on a case-by-case basis by approval authorities.

(3) All personnel involved in the operation of a PDS will have a security clearance at least equal to the highest classification for which the PDS has been approved.

(4) Individuals who must be granted access to any portion of a PDS, but who do not meet the security clearance requirement, must be under surveillance by appropriately cleared and, where available, technically qualified personnel.

(5) All personnel who will guard and/or inspect the PDS will be cleared for the highest classification for which the PDS has been approved. Guards may be stationary or roving patrols, but must be assigned to the PDS areas and not merely assigned as building guards.

(6) Areas in which a PDS is installed will have either protective perimeter construction (with a minimum number of entry points secured or under direct control at all times) or be under the surveillance of a guard or patrol.

(a) Floors, ceilings, walls, doors, windows, and vents will be constructed or installed to prevent clandestine entry. Air conditioning, heating, and other ducts will be provided protection against access by unauthorized individuals and will be provided acoustical treatment.

(b) Vertically adjacent areas in which PDS will be operated are considered separate areas on each floor. An exception is when stairwells are located entirely within the perimeters of the areas subject to the same security safeguards.

(7) PDS, other than fiber optic cables, will be physically and electrically isolated from unprotected distribution systems to prevent inadvertent coupling to unprotected distribution systems. After a PDS has been approved, instances of improper operation or cross talk on circuits will be reported immediately to maintenance and security personnel for corrective action. The part of the system affected will be shut down until the trouble is eliminated.

(8) The passage of PDS through walls, floors, and ceilings will be made at right angles to the plane of the surface. The passage will be through a pipe or other sleeve of sufficient size to permit visual inspection.

(9) Cables and equipment will be inspected by technically qualified personnel (such as C–E installation teams or maintenance personnel) immediately before approval and at frequent irregular intervals after approval.

(10) PDS must be accessible throughout its entire run to permit physical inspection and surveillance. PDS should not be marked or otherwise specifically identified in unrestricted areas.

(11) Subscriber sets used in PDS will be clearly marked with the highest classification for which the circuit has been approved.

(12) The provisions of AR 530–4 and TB 530–1 will be adhered to as appropriate. The installation of all equipment and interconnecting cables will be accomplished in accordance with the TEMPEST criteria for RED circuits.

(13) All cables and wires present in PDS terminals will be fully identified. All extraneous wiring will be removed if possible. Spare communications cables and electric power lines which cannot be removed will be terminated in accordance with TEMPEST standards. This does not include fiber optic cables.

(14) A general starting point for PDS design is a ferrous conduit distribution (FCD) system as described below:

(a) The FCD system must terminate in a terminal box installed within a restricted area at each end of the system.

(b) A completed FCD system should form a single tube from terminal box to terminal box. This will insure that access to PDS cables between terminal boxes cannot be obtained without physically drilling or cutting.

(c) FCD systems should be constructed of rigid, threaded, thickwall ferrous conduit or pipe using elbows, couplings, nipples, and connectors of the same material.

(d) All connections in a FCD system should be clean threaded joints securely tightened and welded completely around all mating surfaces, including both ends of a coupling.

(e) For turns in FCD systems, elbows are preferred over pull boxes. If pull boxes are used, the pull box cover must be attached to the pull box with a continuous weld completely around the mating surface. Boxes equipped with locked or removable covers must be approved by the local INSCOM support element.

(f) With the concurrence of all approval authorities, two or more PDS cables may be carried through the same FCD. If required to serve areas of different classification levels, the cables will be separated in the restricted area with the highest classification level for further routing.

(15) Intrusion-resistant cable (IRC) is another design technique for PDS. Two design approaches for IRC are alarmed cables and hardened cable paths. IRC frequently use an FCD as the design starting point and apply hardening (such as reinforced concrete) and/or technical design techniques, to meet portions of the physical protection and surveillance requirements. The criteria for FCD systems also apply to IRC systems. Additional IRC considerations are as follows:

(a) Developmental work has been performed and is continuing on alarmed cable (wire or fiber optic) systems. Currently, no alarm system has been considered adequate as the only security measure for an IRC. Hardening and/or surveillance are still required. Approval for use of alarmed cables as an IRC in a PDS, and their specifications, is the joint responsibility of the engineering agency and the PDS approval authority.

(b) Fiber optic cables by themselves do not meet the criteria for an IRC. However, fiber optic cables may be used in lieu of wire lines in FCD systems or IRC systems.

(c) Physical protection must be provided for any hardened cable paths in areas which may be within normal reach or easy access of unauthorized personnel. Techniques should be chosen to provide a penetration delay factor. This delay factor will be commensurate with the expected detection time for an intrusion attempt. The technique providing the delay factor should reduce vulnerability to sabotage and provide added physical protection in areas where inadvertent damage to the IRC system may occur.

(d) Frequent inspections of the cable path should be conducted at irregular intervals.

(16) Prior to construction of an FCD or IRC, concurrence of the INSCOM local support element should be obtained by the engineering agency for the proposed overall plan and general installation techniques.

g. Requests for approval of PDS will be submitted through channels to the appropriate approval authority. Requests will be classified CONFIDENTIAL as a minimum and will contain the following information:

(1) Full identification and location of the requesting organization.

(2) A statement of the classification of information to be transmitted over the PDS.

(3) A copy of the building floor plan (or a diagram of the field area, as appropriate) designating the following:

(a) Proposed cable route and location of subscriber sets, distribution frames, keyers, junction boxes, and any other components associated with the circuit.

(b) Other wiring along the PDS route.

(4) Description of the cable installation; for example, 24 pair shielded cable in rigid steel conduit, 6 pair shielded cable in floor or cells, and fiber optic cable. Specify the manner in which the cable will be installed; for example, exposed on the ceiling, or suspended below the false ceiling or on the wall. Indicate the length of the cable runs.

(5) A description including nomenclature of terminal and subscriber equipment to be used.

(6) The clearance status of individuals having access to circuit.

(7) Type of guards, (for example, US Military, US civilian, foreign civilian) and their clearance status.

(8) Description of access control and surveillance of uncleared personnel who may be allowed entry into the area housing any part of the PDS.

(9) Identification of the power source to be used for the PDS and a statement of the distance to the nearest point where undetected tampering would be possible.

(10) A statement that teletypewriter circuits will or will not use low-level keying and signaling. This statement is not applicable to fiber optic circuits.

(11) A justification for use of the proposed PDS.

(12) A statement concerning deviations, if any, from the criteria outlined in paragraph B–3*b*(6) and an evaluation of the inherent security implications.

B–6. Tactical PDS

a. Authority to approve circuits for clear text electrical transmission of SECRET and CONFIDENTIAL information in tactical environments is delegated to commanders of battalion and higher echelons. Under

combat conditions, commanders may subdelegate this authority to the company level. Tactical PDS will not be approved for clear text transmission of TOP SECRET information.

b. The security risk involved in clear text transmission of transitory tactical information is less than that involved in long-term strategic information. In many cases, the value of the tactical information perishes before it can be acted upon by an adversary. Therefore, the risk evaluation should be performed and predicated on the ability of the command to prevent exploitation attempts in a tactical environment and to eliminate or disrupt any such attempts that are initiated.

c. Tactical PDS must meet the following criteria:

(1) Routine transmission of clear text classified information is not authorized until the PDS has been approved.

(2) PDS will be located entirely within the limits of the installation or command post or in areas directly under the using commander's physical control. PDS will not include lines which run outside of the area where the using commander can maintain positive physical control of the lines.

(3) Security techniques will be evaluated on a case-by-case basis by approval authorities.

(4) All personnel involved in the operation of the PDS will have a security clearance at least equal to the highest classification for which the PDS has been approved.

(5) Individuals who must be granted access to any portion of a PDS, but who do not meet the security clearance requirement, must be under surveillance by appropriately cleared and, where available, technically qualified personnel.

(6) The area surrounding the PDS will have either protected perimeters or be under the surveillance of guards or patrols.

(7) PDS will be electrically isolated from unprotected distribution systems to prevent inadvertent coupling to unprotected distribution systems. All wires present in a PDS terminal will be identified. Other communication lines will be separated from the protected circuits and all extraneous wiring will be removed to the maximum extent possible.

(8) Subscriber sets of PDS will be clearly marked with the highest classification for which the circuit has been approved.

(9) The use of single-wire circuitry using the earth, or the chassis of equipment, or the shields of the conductors as a return path will not be used for PDS.

(10) After a PDS has been approved, instances of improper operation or cross talk on circuits will be reported immediately to maintenance personnel and security personnel for corrective action. The part of the system which is affected will be shut down until the trouble is eliminated.

(11) Cables and equipment at PDS terminals will be inspected for physical taps and other evidence of tampering immediately before approval and at frequent irregular intervals after approval by technically qualified personnel.

(12) The criteria contained in *(c)* may be waived by the approval authority during hostilities.

d. Formal request for and approval of tactical PDS may be eliminated at the discretion of the approval authority concerned. Approvals may be granted in any form at the discretion of the approval authority. Approvals should be based on the following information, which will be classified CONFIDENTIAL when associated with a specific PDS.

(1) Description of the PDS.

(2) Classification level of the information to be transmitted.

(3) An evaluation of the security risk involved.

(4) Standing operating procedures (SOP) and installation parameters.

e. Telecommunications systems in the tactical environment may be designed or combined into many configurations. Yet, the underlying national policy is unchanged; that is, a classified information electrically transmitted over telecommunications systems must be secured by approved cryptosystems or by PDS. Care must be exercised to prevent the compromise of classified information through inadequate surveillance or physical protection or through improper installation and operation of PDS or combined systems.

(1) Field telephones, their wirelines and switchboards, within a tactical command post (CP) may be established as PDS. The simplest case is a tactical CP established in a rural area where circuits are not connected or connectable outside the CP. In these situations, positive physical control and surveillance of PDS wirelines and cables is easiest to maintain.

(2) A tactical CP established in urban areas increases the difficulty of establishing and maintaining physical control and surveillance of PDS wirelines and cables. More care in separation of PDS from existing wires, and posting of guards with visual surveillance and/or frequent guard patrols may be necessary.

(3) A tactical CP dispersed throughout a wide area, (for example, several villages used to house elements of the CP) may still permit establishment of a PDS. However, the increased distances and wider dispersion further increase the difficulties of maintaining physical control and surveillance. In such cases the possibility of hostile forces operating within friendly areas of control must be considered. Guard forces protecting and patrolling such PDS should be familiar with wiretap techniques and schedule frequent but irregular patrols of all PDS wirelines and cable runs. Operators and maintenance personnel must be alert to any abnormal operation of the PDS.

(4) To reduce or alter the electromagnetic profile of a CP, radio transmitters may be dispersed and remoted some distance from their CP. Wirelines and cables linking the CP to remote radio transmitters can only be considered for PDS if the radio transmitters or connecting cables are secured by approved COMSEC equipment. When the COMSEC equipment is available to secure the radio transmitters, the circuits to the radio transmitter may be established as PDS; considerations and criteria for PDS within the CP (rural, urban or dispersed) apply.

Appendix C
Authentication Systems

C-1. General

Authentication systems prevent unauthorized stations from entering friendly radio nets to disrupt or confuse operations. They also protect a communications system against false transmissions (imitative deception). The only authentication systems authorized for use in the US Army are those produced by NSA, or, for an emergency requirement, by INSCOM. If a special or emergency requirement arises, the unit commander must notify the controlling authority of the authentication system in use or the controlling authority's designated representative (C-E Officer).

C-2. Instructions

The two methods of authentication that are authorized for use are shown below. The operational distinction between the two is that challenge and reply requires two-way communications, whereas transmission authentication does not.

a. Challenge-reply authentication. In challenge-reply authentication, the called station always gives the first challenge. This challenge and reply method validates the authenticity of the calling station. It also prevents an unauthorized operator from entering a net to obtain authentication responses for use in another net. The station making the call may counterchallenge the called station, using a different challenge. Only the station responding to a challenge is verified. Do not accept a challenge as an authentication.

(1) If an incorrect reply is received or if an unusual (15 to 20 seconds) delay occurs between the challenge and the reply another challenge should be made.

(2) Operators will occasionally misauthenticate by using the wr· ıg system or misreading the table. In such cases, the challenging station should attempt to pinpoint the difficulty and then rechallenge.

(3) Never give the challenge and reply in the same transmission (self-authentication).

b. Transmission authentication. This is a method used by a station to authenticate a message. It is used when challenge-reply authentication is not possible; for example, when a station is under radio listening silence. Transmission authentication differs from self-authentications in that authenticators are either carefully controlled to insure one-time use or are time based.

C-3. When to authenticate

Challenge and reply or transmission authentication systems, as appropriate, will be used when—

a. A station suspects imitative deception on any circuit.

b. A station is challenged to authenticate. Stations will not respond to a challenge when under an imposed radio listening silence.

c. Directing radio silence, radio listening silence, or requiring a station to break an imposed silence. (Transmission authentication).

d. Transmitting contact and amplifying reports in plain language.

e. Transmitting operating instructions that affect the military situation. Examples are closing down a station or watch, changing frequency other than normal scheduled changes, or directing establishment of a special communications guard. Other examples are requesting artillery fire support or directing relocation of units.

f. Transmitting a plain language cancellation.

g. Making initial radio contact or resuming contact after prolonged interruptions.

h. Transmitting to a station under radio listening silence (transmission authentication).

i. Authorized to transmit a classified message in the clear.

j. Forced, because of no response by the called station, to send a message in the blind (transmission authentication).

C-4. Exceptions

Authentication is not required under the following conditions:

a. When using authorized on-line cryptosystems, unless it is suspected that the cryptonet has been compromised.

b. When making initial contact after a scheduled call sign and frequency change, since only bona fide stations should know their assigned call sign and frequency for the time period in use.

Glossary

Section I
Abbreviations

ACCLAIM
Army COMSEC Commodity Logistics Accounting Information Management System

ACCOR
Army COMSEC Central Office of Record

ACSI
Assistant Chief of Staff for Intelligence

ARNG
Army National Guard

AUTOSEVOCOM
automatic secure voice communications

BOIP
basis of issue plan

CEARS
COMSEC equipment asset reporting system

CEMA
COMSEC equipment modification application

CEOI
communications electronics operation instructions

COMINT
communications intelligence

COMSEC
communications security

CONUS
Continental United States

CP
command post

CRE
COMSEC research and engineering coordination

CRP
COMSEC Resource Program

DARCOM
United States Army Material Development and Readiness Command

DCS
Defense Communications System

DCSLOG
Deputy Chief of Staff for Logistics

DCSOPS
Deputy Chief of Staff for Operations and Plans

DCSPER
Deputy Chief of Staff for Personnel

DCSRDA
Deputy Chief of Staff for Research, Development, and Acquisition

DES
Data Encryption Standard

DIRNSA
Director, National Security Agency

EAC
echelons above corps

ECM
electronic countermeasures

EMSEC
emissions security

EW
electronic warfare

FDTE
force development testing and experimentation

FORSCOM
United States Army Forces Command

HQDA
Headquarters, Department of the Army

HSC
United States Army Health Services Command

ILS
Integrated Logistics Support

INSCOM
United States Army Intelligence and Security Command

LOA
letter of agreement

MACOM
major Army command

NCSC
National Communications Security Committee

NICP
national inventory control point

NMP
national maintenance point

NSA
National Security Agency

NSC
National Security Council

OCO
operational capability objective

OCONUS
Outside the Continental United States

O&M
operations and maintenance

O&O
operational and organizational

OPA
other procurement, Army

OPSEC
operations security

OSD
Office of the Secretary of Defense

OT
operational test

OTEA
Operational Test Evaluation Agency

PDS
protected distribution system

RDTE
research, development, test and evaluation

ROC
required operational capability

SECDEF
Secretary of Defense

SIGINT
signals intelligence

SIGSEC
signal security

TELER
telecommunications requirement

TOE
table of organization and equipment

TRADOC
United States Army Training and Doctrine Command

USACC
United States Army Communications Command

USAR
United States Army Reserve

USAREUR
United States Army, Europe

WESTCOM
United States Army Western Command

COMSEC Resources Program
Includes all resources and manpower concerned with or in support of the communications security (COMSEC) efforts of the Army.

COMSEC surveillance
The systematic examination of telecommunications to determine the adequacy of COMSEC measures, to identify COMSEC deficiencies, to provide data from which to predict the effectiveness of proposed COMSEC measures, and to confirm the adequacy of such measures after implementation.

Protected distribution system (PDS) (formerly called an "approved circuit.")
A wireline or fiber optics system which includes adequate acoustical, electrical, electromagnetic, and physical safeguards to permit its use for the transmission of unencrypted information.

Telecommunications
Any transmission, emission, or reception of signs, signals, writing, images, and sounds or information of any nature by wire, radio, visual, or other electromagnetic systems.

Record information
All forms (e.g., narrative, graphic, data, computer memory) of information registered in either temporary or permanent form so that it can be retrieved, reproduced, or preserved.